

5

10

15

20

25

FIELD OF THE INVENTION

The present invention relates generally to systems and methods for controlling network access, and more particularly, to systems and methods for establishing dynamic user network access.

5

BACKGROUND OF THE INVENTION

User access to computer networks has traditionally been based upon a two step authentication process that either provides a user total network access, or refuses the user any access whatsoever. In the first step of the process, a user establishes a communication link with a network via a telephone line, dedicated network connection (e.g., Broadband, Digital Signal Line (DSL)), or the like. In the second step of the authentication process, the user must input identification information to gain access to the network. Typically, the input identification information includes a user name and password. Using this information, the network or service provider verifies that the user is entitled to access the network by determining whether the identification information matches subscriber information contained in a subscriber table (or database) that stores identification information for all users authorized to access the network. Where user input information matches subscriber data in the subscriber table, the user is authorized to access any and all services on the network. On the other hand, if the user input identification information fails to match subscriber data in the table, the user will be denied access to the network. Thus, once a user's identity is compared to data stored within a subscription table, the user is either entitled network access, or denied access altogether. Furthermore, where the user is authorized access to the network, the user is typically authorized to access any destination accessible via the network. Therefore, conventional authentication of users is based on an all-or-nothing approach to network access.

In many conventional network access applications, such as in conventional Internet access applications, the subscriber database (or table) not only stores data corresponding to the identity of subscribers authorized to access the network, but also stores information that can vary based upon the particular subscriber. For instance, the subscriber database can include subscriber profiles that indicate the type of access a

00693060-102000

5

10

20

25

to particular sites. In addition to authorizing user access to a network, it would be advantageous for a network, such as an ISP or enterprise network, to selectively permit users a range of authorization, such that the user's access is not based upon an all or nothing approach.

5

SUMMARY OF THE INVENTION

The present invention includes a method and system for selectively implementing and enforcing Authentication, Authorization and Accounting (AAA) of users accessing a network via a gateway device. According to the present invention, a user may first be

10 authenticated to determine the identity of the user. The authentication capability of the system and method of the present invention can be based upon a user ID, computer, location, or one or more additional attributes identifying a source (e.g., a particular user, computer or location) requesting network access. Once authenticated, an authorization capability of the system and method of the present invention is customized based upon

15 the identity of the source, such that sources have different access rights based upon their identity, and the content and/or destination requested. For instance, access rights permit a first source to access a particular Internet destination address, while refusing a second source access to that same address. In addition, the authorization capability of the system and method of the present invention can be based upon the other information

20 contained in the data transmission, such as a destination port, Internet address, TCP port, network, or similar destination address. Moreover, the AAA of the present invention can be based upon the content type or protocol being transmitted. By authenticating users in this manner, each packet can be filtered through the selective AAA process, so that a user can be identified and authorized access to a particular destination. Thus, each time the

25 user attempts to access a different destination, the user is subject to the AAA, so that the user may be prevented access from a particular site the AAA system and method deem inaccessible to the user based upon the user's authorization while permitting access to other sites that the AAA method and system deem accessible. Additionally, according to one embodiment of the invention, source access to the network may be tracked and

30 logged by the present invention for accounting and historical purposes.

According to yet another aspect of the invention, the method includes updating
25 the source profile database when a new source accesses the network. Additionally, the
method can include maintaining in the source profile database a historical log of the
source's access to the network. Moreover, the attribute associated with the source can be
based upon a MAC address, User ID or VLAN ID associated with the source computer
from which the request for access to the network was transmitted. According to yet
30 another aspect of the invention, receiving at the gateway device a request from a source
for access can include the step of receiving a destination address from the source.

According to another embodiment of the invention, there is disclosed a system for selectably controlling and customizing access, to a network, by a source, where the source is associated with a source computer, and wherein the source computer has transparent access to the network via a gateway device and no configuration software
5 need be installed on the source computer to access the network. The system includes a gateway device for receiving a request from the source for access to the network, and a source profile database in communication with the gateway device and located external to the gateway device, wherein the source profile database stores access information identifiable by an attribute associated with the source, and wherein the attribute is
10 identified based upon a data packet transmitted from the source computer and received by the gateway device. The system also includes a AAA server in communication with the gateway device and source profile database, wherein the AAA server determines if the source is entitled to access the network based upon the access information stored within the source profile database, and wherein the AAA server determines the access rights of
15 the source with the access rights defining the rights of the source to access destination sites via the network.

According to one aspect of the invention, the packet received by the gateway device includes at least one of VLAN ID, a circuit ID, and a MAC address. Additionally, according to another aspect of the invention, the source profile database includes a
20 remote authentication dial-in user service (RADIUS) or a lightweight directory access protocol (LDAP) database. Furthermore, the source profile database can include a plurality of source profiles, wherein each respective source profile of the plurality of source profiles contains access information. According to the invention, each respective source profile can also contain historical data relating to the duration of network access
25 for use in determining the charges due for the network access. According to yet another aspect of the invention, the source profile database can be located within the AAA server.

According to another embodiment of the present invention, there is disclosed a method for redirecting a source attempting to access a destination through a gateway device, wherein source is associated with a source computer, and wherein the gateway
30 device enables the source to communicate with a network without requiring the source computer to include network software configured for the network. The method includes

receiving at the gateway device a request from the source to access the network,
 identifying the source based upon an attribute associated with the source, and accessing a
 source profile database located external to the gateway device, where the source profile
 database stores access rights of the source. The method further includes determining the
 5 access rights of the source based upon the identification of the source, wherein the access
 rights define the rights of the source to access destination sites via the network.

According to one aspect of the invention, accessing a source profile database
 includes accessing a source profile database that includes a remote authentication dial-in
 user service (RADIUS), or a lightweight directory access protocol (LDAP) database.
 10 According to another aspect of the invention, the method can include assigning a location
 identifier to the location from which requests for access to the network are transmitted,
 wherein the location identifier is the attribute associated with the source. The method can
 also include updating the source profile database when a new source accesses the
 network, and maintaining in an accounting database a historical log of the source's access
 15 to the network, wherein the accounting database is in communication with the source
 profile database.

According to yet another aspect of the invention, receiving at the gateway device
 a request from a source for access can include the step of receiving a destination address
 from the source. Moreover, determining if the source computer is entitled to access the
 20 destination address can further include denying the source computer access where the
 source profile indicates that the source computer is denied access. Determining if the
 source is entitled to access the network can also further include directing the source to a
 login page when the source profile is not located within the source profile database.

According to yet another embodiment of the invention, there is disclosed a system
 25 for enabling transparent communication between a computer and a service provider
 network. The system includes a computer, and a network gateway device in
 communication with the computer for connecting the computer to a computer network,
 where the network gateway device receives source data that represents a user attempting
 to access said computer network. The system also includes a service provider network in
 30 communication with the network gateway device, where the service provider network
 includes an authentication server located external to the network gateway device and in

5

10

20

FIG. 2 is a flow chart of a method in which a AAA server performs authentication, authorization, and accounting, according to one aspect of the invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

The present invention now will be described more fully hereinafter with reference
10 to the accompanying drawings, in which preferred embodiments of the invention are
shown. This invention may, however, be embodied in many different forms and should
not be construed as limited to the embodiments set forth herein; rather, these
embodiments are provided so that this disclosure will be thorough and complete, and will
fully convey the scope of the invention to those skilled in the art. Like numbers refer to
15 like elements throughout.

Referring now to FIG. 1, a computer system 10 is illustrated in block diagram form. The computer system 10 includes a plurality of computers 14 that can communicate with one or more online services 22 or networks via a gateway device 12 providing the interface between the computers 14 and the various networks 20 or online services 22. One embodiment of such a gateway device has been described in U.S. Patent Application No. 08/816,174 (referred to herein as the Gateway Device Application), the contents of which are incorporated herein by reference. Briefly, the gateway device 12 facilitates transparent computer 14 access to the online services 22 or networks 22, such that the computers 14 can access any networks via the device 12 regardless of their network configurations. Additionally, the gateway device 12 includes the ability to recognize computers attempting to access a network 12, the location of computers attempting to access a network, the identity of users attempting to gain network access, and additional attributes, as will be discussed below with respect to the dynamic AAA methods and systems of the present invention.

30 As illustrated in FIG. 1, the computer system 10 also includes an access concentrator 16 positioned between the computers 14 and the gateway device 12 for

5

10

15

25

5

10

20

individual rights of each user, as the rights are associated with the computer (e.g., identified by MAC address), rather than with the respective users.

The authentication of sources via an attribute associated with the source is performed by the AAA server 30, illustrated in FIG. 1. The AAA server 30 stores source profiles corresponding to sources identified by the AAA server 30. According to one aspect of the present invention, the AAA server 30 is located entirely within the gateway device 12. According to another aspect of the invention, the AAA server 30 can comprise a plurality of components, at least some of which are external to the gateway device 12, or alternatively, the AAA server 30 can be located entirely external to the gateway device 12. For example, the location of the AAA server 30 may be such that the gateway device 12 communicates with the AAA server 30 via internet protocol. According to one embodiment of the invention, the AAA server 30 can be maintained by an ISP, which identifies sources authorized to communicate with the network via the ISP. Therefore, it will be appreciated that the AAA server 30 may be located at any internet address and stored on any computer accessible via internet protocol.

According to one aspect of the invention, a separate source profile exists for each source accessing the system. Source profiles are maintained in a source profile database, which may be an internal component of the AAA server 30, an external component of the AAA server 30, or a separate component in communication with the AAA server 30. Preferably, the source profile database is located external to the gateway device and network to alleviate administrative burden on the network so that the network does not have to set up and maintain separate authentication databases on each network or gateway device. This is also preferable because each gateway device 12 allows a finite number of users to access the network, which requires multiple gateway devices to accommodate a large number of sources. Secondly, administering and maintaining one consolidated database of authentication data is easier than multiple smaller databases. Lastly, locating the source profile database external to the local network can allow an ISP or third party provider to maintain the confidentiality of the information stored within the database and maintain and control the database in any manner the third party provider so desires.

The source profile database may comprise programmable storage hardware or like means located on a conventional personal computer, mainframe computer, or another suitable storage device known in the art. Additionally, the means for comparing the received data to the data within the database can comprise any software, such as an executable software program, which can compare data. For example, the AAA server 30 may store source profiles on a hard drive of a personal computer, and the means for comparing the received source data to the source profiles resident on the computer can include computer software, such as Microsoft Excel (Microsoft Excel is a trademark of Microsoft Corporation, Redmond, Washington). According to another embodiment of the invention, the AAA server 30 or source profile database can comprise a Remote Authentication Dial-In User Service (RADIUS) or a Lightweight Directory Access Protocol (LDAP) database, which are well known to those of skill in the art.

ATL01/10823107v2

According to another aspect of the invention, where the source cannot be identified, the source may be directed to a login page in order to gather additional information to identify the source. For instance, the information may be entered with the aid of a webpage, a pop-up control panel or user interface, which can open when the source initially connects to the gateway device 12, as effectuated by a home page redirection capability, described herein and in U.S. Patent Application, Serial No. 09/458,569, filed December 8, 1999, entitled "Systems And Methods For Redirecting Users Having Transparent Computer Access To A Network Using A Gateway Device Having Redirection Capability" (referred to hereinafter as the "Redirection Application"), in U.S. Patent Application, Serial No. 09/458,579, filed December 8, 1999, entitled "Systems And Methods For Redirecting Users Having Transparent Computer Access To A Network Using A Gateway Device Having Redirection Capability," and in U.S. Patent Application, Entitled "Systems and Methods for Redirecting Users Attempting to Access a Network Site," filed concurrently herewith, inventors Joel Short and Florence Pagan, the contents of each of which are incorporated herein by reference.

According to one aspect of the invention, the AAA server 30 can identify the source in communication with the gateway device in a manner that is transparent to computer users. That is, according to one aspect of the invention, a user will not be required to input identification information, reconfigure the source computer or otherwise change the source computer's primary network settings. Furthermore, no additional configuration software will have to be added to the source computer. After a packet is received by the gateway device, attributes identified by the data packet can be compared with the data contained in the source profile database. Therefore, in addition to not requiring the reconfiguration of computers accessing the network, AAA servers of the present invention have the ability to authenticate sources without requiring interactive steps by the computer user, such as the entering of a user ID. For instance, the AAA server 30 may automatically identify the source based upon a MAC address, so that authorization of the source can be readily determined. Therefore, it will be appreciated that the AAA server 30 can determine the user, computer, or location from which access is requested by comparing the attributes associated with the received data packet (such as in a header of the data packet) with data drawn from the source profile database. As will

09693060-100000

be described below, the access rights associated with the source may also be stored within the source profile database so that the system and method of the present invention can dynamically authorize access to particular services or destinations.

Once the source has established the network service connection via the authentication process discussed above, and a tunnel has been opened to facilitate a communication line between the source computer and a network, the gateway device 12 communicates with the AAA server 30 to assemble source profile information, or source-specific data. The source profile information that the gateway device assembles may include a MAC address, name or ID, circuit ID, billing scheme related data, service level data, user profile data, remote-site related data, and like data related to the source. As such, the AAA server 30 can transmit to the gateway device 12 any requisite information relating to the source's authorization rights and use of the network, as is next explained in detail.

In addition to authenticating users, the AAA server 30 of the present invention provides an authorization function, in which the source access rights are determined. The present invention enables dynamic authorization of sources, such that each source might have different respective network usage or access rights. After authentication, the AAA server 30 compares the attributes of the source with the access rights of the source associated with the user, computer, location or attribute(s). The access rights may be stored within the source profile database or within a separate subscription database located internal or external to the gateway device 12. Therefore, separate databases may be utilized, where one stores identification information on sources for authentication, and another database stores the access rights of those sources that have been authenticated. However, because the profiles of all sources, identified by attribute or a combination of attributes, are stored in a source profile database, it may be advantageous to locate information regarding access rights in the source profile database, which already contains information regarding each authenticated source, as described above.

According to one aspect of the invention the source profile database stores information defining the access rights of a source. For example, a source profile database may contain information indicating that a source having a particular MAC address has purchased pre-paid access, or that a given circuit ID has free access or unlimited access.

Guests in a particular room or rooms of a hotel, for example, suites and penthouses, may receive free unlimited Internet access. Therefore, access rights can be available contingent upon the source's location (e.g. room) or location status (e.g. suite). In this event, no further identification is required, as the location from which the source is requesting access is known to the gateway device and stored in the source profile database.

In addition to storing information concerning what each source is authorized to access, the source profile database can also include specialized access information associated with a particular source, such as the bandwidth of the source's access, or a homepage to which the source should be directed. For example, a user accessing the network from a penthouse may receive a higher access baud rate than someone accessing the network from a typical hotel room. For example, where a user is transparently accessing the gateway device from a hotel room, the hotel network administrator may enter user access information into the source profile database based upon access rights associated with a room in the hotel. This can also be done automatically by the gateway device or a local management system, such as a hotel property management system, when the user checks into his or her room. Additionally, the user may establish the information to be contained within the source profile database upon first accessing the gateway device. For instance, a new user may be directed to enter a credit card number, e-wallet account information, pre-paid calling card number or like billing information to obtain access to the system. A source profile can also include historical data relating to a source's access to the network, including the amount of time a source has accessed the network. Specialized access or accounting information contained within the source profile database may be established by the system administrator, or by the source who has purchased or otherwise established access to the network.

According to one aspect of the invention, the authorization capability of the AAA server 30 can be based upon the type of services the source is attempting to access, such as a destination address, identified by the gateway device 12 based upon data received from the source computer. The destination can be a destination port, Internet address, TCP port, network, or the like. Moreover, the authorization capability of the AAA server 30 can be based upon the content type or protocol being transmitted. According to the

20

25

Once a source profile has been determined by accessing the authorization rights stored in the source profile database, three possible actions can result. Specifically, once a source's authorization rights have been retrieved the AAA server **30** may determine a source to have access **222**, to be pending or in progress **224**, or to not have access **226**. First, a source is deemed valid (i.e., to have access) where the source profile database so states. If a source is determined to be valid, the source's traffic can be allowed to proceed out of the gateway device to the networks or online services the user associated with the source wishes to access (block **230**). Alternatively, the source may be redirected to a portal page, as described in the Redirecting Application, prior to being allowed access to the requested network. For example, a user may be automatically forwarded to a user-input destination address, such as an Internet address, for example, where a user has free access associated with the user's hotel room. Alternatively, this may occur where the user has already purchased access and the user has not exhausted available access time. Furthermore, an accounting message may be initiated **230** to log the amount of time the user is utilizing the gateway device such that the user or location may be billed for access.

ATL01/10823107v2

have access 226 so that the user is not permitted to access a destination via the network (block 260).

Referring now to the accounting function of systems and methods of the present invention, upon authorizing a source network access, the AAA server 30 can register an accounting start to identify that the source is accessing the network. Similarly, when the source logs off or terminated the network session, an accounting stop can be registered by the AAA server 30. Accounting starts or stops can be identified by the gateway device 12 or by the AAA server 30 upon a source's authentication or authorization to access a desired destination. Furthermore, accounting starts or stops can be registered in the source profile, or can be stored in a database separate from the AAA server 30 and located external to the network. Typically, accounting starts and stops include time stamps that indicate the amount of time a source has been accessing the network. Using this data, the time between the accounting start and accounting stop can be tallied so that the source's total connection time may be computed. Such information is valuable where the source is charged by an increment of time, such as an hour. A billing package, as are well known in the art, could then tally a user's total time accessing the network over a set period, such as each month, so that a bill can be created for the source. Because networks and ISPs often may charge a set rate for a specific duration of time (i.e., flat rate pricing), such as a month, regardless how much time is being spent accessing the network, accounting stops and starts may not be required for billing purposes. Nevertheless, accounting starts and stops may generally be recorded by the network provider or ISP for usage statistics.

An ISP or similar access provider would additionally benefit from being able to track subscriber's use of the ISP to establish bills, historical reports, and other relevant information. Preferably, the AAA server 30 is in communication with one or more processors for determining any fees which may be charged to the source, or due from the source, for network access or services. The AAA server 30 retrieves the historical accounting data in a real time basis or after a specific interval of time has elapsed. Preferably, the AAA server 30 retains such data in an easily accessible and manipulatable format such that the access provider (e.g., ISP) can produce reports representative of any desired type of historical data. For example, to project future use of the access provider,

5

15

25